UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/957,415	09/20/2001	Scott Thomas Elliott	RPS9 2001 0044	3264

47052 7590 05/26/2005		EXAMINER
SAWYER LAW GROUP LLP		CHAI, LONGBIT
PO BOX 51418		

ART UNIT	PAPER NUMBER
2131	

PALO ALTO, CA 94303

DATE MAILED: 05/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/957,415	ELLIOTT ET AL.
	Examiner	**Art Unit**	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *13 May 2005*.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☐ Claim(s) _____ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-22* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on *9/20/2001* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1 – 19 have been presented for examination. New claims 20 – 22 have

been added in an amendment filed 5/13/2005. Therefore, presently pending claims are

1 – 22.

Response to Arguments

2.   Applicant's arguments filed on 5/13/2005 with respect to the subject matter of the

instant claims have been fully considered but are not persuasive.

3.   As per claim 1, 7 and 16, Applicant remarks: "Ansell in view of Christensen fail to

teach or suggest storing tag data along with key material in conjunction with using the

tag data to determine whether the key material is bound to the system". Examiner

notes Applicant's arguments have been fully considered but are not persuasive.

Examiner notes key material is interpreted as an integrated data collection of security

keys information kept in a passport data structure, which can represent either a

machine-binding or a user-binding (Ansell: Column 2 Line 33 – 35) combining with a

user option indicator selecting either machine-binding or a user-binding passport

(Ansell: Column 3 Line 10 – 12). Thereby, Examiner notes the collection of security key

passport data structures combining with user option indicator is equivalent to the key

material including tag data to meet the claim language. Although the claims are

interpreted in light of the specification, limitations from the specification are not read into

the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1 – 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Ansell (Patent Number: 6792113), hereinafter referred to as Ansell, in view of

Christensen (Patent Number: 2002/0071559), hereinafter referred to as Christensen.

As per claim 1, 7 and 16, Ansell teaches a method for control of key pair usage in

a computer system, the method comprising:

Ansell teaches creating key pair material and determining whether the key pair

material is bound to the hardware ID (i.e. machine binding) (Ansell: se for example,

Figure 3B Element 140, 2404 & 308 and Column 2 Line 33 – 64 and Column 10 Line 10

– 25).

Ansell further teaches the security key pair can be associated with either the type

of a machine-binding (i.e. binding with HW ID) data structure (Ansell: se for example,

Figure 3B) or the type of a user-binding (i.e. non-binding with HW ID) data structure

(Ansell: se for example, Figure 3A).

Ansell does not disclose expressly creating key pair material for utilization with

an embedded security chip of the computer system.

Christensen teaches creating key pair material for utilization with an embedded

security chip of the computer system (Christensen: see for example, Paragraph [0245]

and [0252] Line 1 – 4: Christensen teaches the secured HW ID can be stored in the

embedded chip).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Christensen within the system of Ansell

because (a) Ansell teaches the machine-binding hardware ID is used for the decryptor

and is stored as read-only data (Ansell: see for example, Figure 3B Element 140 & 308

and Column 6 Line 5 – 12) and (b) Christensen teaches providing a mechanism by

storing the encryption / decryption key in a silicon chip with the advantage that the

decryption key is never exposed to the receiver (Christensen: see for example,

Paragraph [0001] Line 7 – 8 and Paragraph [0255] Line 1 – 2).

Accordingly, Ansell in view of Christensen teaches:

(a) creating key pair material for utilization with an embedded security chip of the

computer system, the key pair material including tag data (Examiner notes the tag data

is interpreted as the indicator to identify the passport data structure as either the type of

a machine-binding structure or the type of a user-binding data structure for the

associated key pairs as addressed above and thereby, the indicator can indeed serve

as the desired tag bit).

(b) determining whether the key pair material is bound to the embedded security

chip based on the tag data (See the same rationale as addressed above).

As per claim 2, 9 and 17, Ansell in view of Christensen teaches the claimed invention as described above (see claim 1, 8 and 16 respectively). Ansell further teaches comprising a bit to indicate whether binding is required for the key pair material (Ansell: se for example, Figure 3B & 3A: Ansell teaches the security key pair can be associated with either the type of a machine-binding (i.e. binding with HW ID) data structure (Ansell: se for example, Figure 3B) or the type of a user-binding (i.e. non-binding with HW ID) data structure (Ansell: se for example, Figure 3A) and thereby using a bit is equivalent to the indicator that the security private key is associated with either one of the presented two different types of binding structure as taught by Ansell).

As per claim 3 and 11, Ansell in view of Christensen teaches the claimed invention as described above (see claim 1 and 7 respectively). Ansell further teaches creating key pair material further comprises creating key pair material of different levels (Ansell: see for example, Figure 3A & 3B: (a) hardware ID key pair in the machine-binding passport data structure (Figure 3B Element 140) is qualified as a hardware key pair level) (b) machine-binding private key in the machine-binding passport data structure (Figure 3B Element 304) is qualified as a platform key pair level (c) user private key in the user-binding passport data structure (Figure 3A Element 304) is qualified as user key pair level and (d) content master key (i.e. application key) is qualified as a credential key pair level).

As per claim 4, 5, 12 and 13, Ansell in view of Christensen teaches the claimed

invention as described above (see claim 3, 4, 11 and 12 respectively). Ansell further

teaches the four levels further comprise a hardware key pair level, a platform key pair

level, a user key pair level, and a credential key pair level (Ansell: see for example,

Figure 3A & 3B: the four levels are (a) hardware ID key pair in the machine-binding

passport data structure (Figure 3B Element 140) is qualified as a hardware key pair

level) (b) machine-binding private key in the machine-binding passport data structure

(Figure 3B Element 304) is qualified as a platform key pair level (c) user private key in

the user-binding passport data structure (Figure 3A Element 304) is qualified as user

key pair level and (d) content master key (i.e. application key) is qualified as a credential

key pair level).

As per claim 6 and 14, Ansell in view of Christensen teaches the claimed

invention as described above (see claim 5 and 13 respectively). Ansell further teaches

including tag data further comprises including a tag for indicating binding is required for

the platform key pair level (Ansell: see for example, Column 10 Line 19 – 25 and

Column 2 Line 33 – 64: the set tag bit for machine-binding private key (interpreted as

the platform key) bound to the embedded security chip is equivalent to the indicator

associated with the machine-binding passport data structure for respective private key).

As per claim 8, Ansell in view of Christensen teaches the claimed invention as

described above (see claim 7). Ansell further teaches comprising means for security

setup to provide an interface on the computer system for administration of the security

processor, including providing the tag data (Ansell: see for example, Column 6 Line 16

– 18).

As per claim 10, Ansell in view of Christensen teaches the claimed invention as

described above (see claim 7).   Ansell in view of Christensen further teaches the

security processor includes memory for storing the key pair material (Ansell: see for

example, Column 8 Line 28 – 31) and (Christensen: see for example, Paragraph [0245]

and [0252] Line 1 – 4).

As per claim 15, Ansell in view of Christensen teaches the claimed invention as

described above (see claim 14).   Ansell further teaches the key pair material further

comprises a tag to indicate binding is not required for the user key pair level (Ansell: see

for example, Figure 3A & Figure 3B: the indicator (tag bit) for the user private key is

inherent to be reset (OFF) as taught by Ansell because the 3rd level of user private key

is transparent to (i.e. not dependent on) the 1st level of HW ID (i.e. embedded security

chip level).

As per claim 18, Ansell in view of Christensen teaches the claimed invention as

described above (see claim 17).   Ansell further teaches utilizing the reset tag bit with a

user key pair level in the hierarchical structure to allow user key pairs to be verified

securely on more than one computer system (Ansell: see for example, Figure 3A &

Figure 3B: the indicator (tag bit) for the user private key is inherent to be reset (OFF) as

taught by Ansell because the 3rd level of user private key is transparent to (i.e. not

dependent on) the 1st level of HW ID (i.e. embedded security chip level) and thereby, it

allows user key pairs to be verified securely on more than one computer system – i.e.

there is no binding with a particular machine / HW ID).

As per claim 19, Ansell in view of Christensen teaches the claimed invention as

described above (see claim 18).   Ansell further teaches utilizing the set tag bit with a

platform key pair level in the hierarchical structure to allow a platform key pair to be

verified only on a computer system where binding with the embedded security chip is

established (Ansell: see for example, Column 2 Line 33 – 64 and Figure 3B: the

machine binding private key (interpreted as the platform key) with the indicator

associated with the machine binding passport data structure allows a platform key pair

to be verified only on a computer system where binding with a particular HW ID).

As per claim 20, 21 and 22, Ansell in view of Christensen further teaches the

hierarchical structure is organized such that key pair material for potion of each of at

least two levels of the hierarchical structure are not bound (Ansell: see for example,

Figure 3A & 3B: the four levels are (a) hardware ID key pair in the machine-binding

passport data structure (Figure 3B Element 140) is qualified as a hardware key pair

level) (b) machine-binding private key in the machine-binding passport data structure

(Figure 3B Element 304) is qualified as a platform key pair level (c) user private key in

the user-binding passport data structure (Figure 3A Element 304) is qualified as user

key pair level and (d) content master key (i.e. application key) is qualified as a credential

key pair level) – Therefore, Examiner notes the user private key level and content

master level of the hierarchical structure are clearly not bound (i.e. at least two levels (c)

& (d)).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

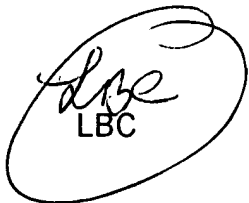than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Longbit Chai whose telephone number is 571-272-3788.

The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100